(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 September 2000 (14.09.2000)

PCT

(10) International Publication Number
WO 00/54491 A1

(51) International Patent Classification[7]: H04M 15/00, 15/06, 1/56

(21) International Application Number: PCT/US00/06195

(22) International Filing Date: 9 March 2000 (09.03.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/265,118 9 March 1999 (09.03.1999) US

(71) Applicant and
(72) Inventor: NOVAK, Don [US/US]; 6916 B N.E. 44th Cir., Vancouver, WA 98661 (US).

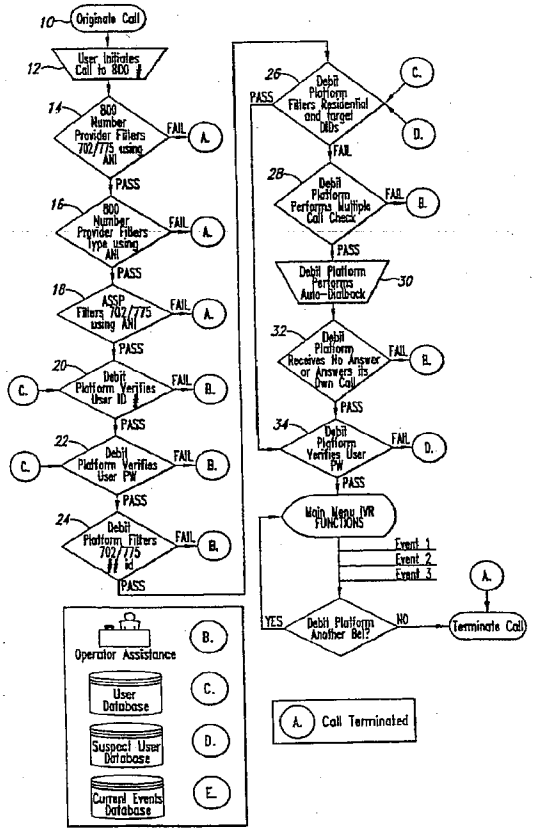
(74) Agent: BECKER, Todd, M.; Davis Wright Tremaine LLP, 2600 Century Square, 1501 Fourth Avenue, Seattle, WA 98101-1688 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PROCESS FOR SCREENING AND TRACKING USERS ON A TELEPHONIC NETWORK



(57) Abstract: A process for screening and monitoring users connecting or attempting to connect from a user platform to a target platform via a telephone network, the target platform being located within a specified jurisdiction. The process comprises filtering unauthorized calls from connecting to a target platform and writing call information for all calls connections made or attempted (step 12-18), verifying user identification (steps 20-34), and establishing a network connection between authorized callers and the target platform.

WO 00/54491 A1

Published:
With international search report.

(48) Date of publication of this corrected version:
5 April 2001

(15) Information about Correction:
see PCT Gazette No. 14/2001 of 5 April 2001, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 September 2000 (14.09.2000)

PCT

(10) International Publication Number
WO 00/54491 A1

(51) International Patent Classification[7]: H04M 15/00, 15/06, 1/56

(21) International Application Number: PCT/US00/06195

(22) International Filing Date: 9 March 2000 (09.03.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/265,118 9 March 1999 (09.03.1999) US

(71) Applicant and
(72) Inventor: NOVAK, Don [US/US]; 6916 B N.E. 44th Cir., Vancouver, WA 98661 (US).

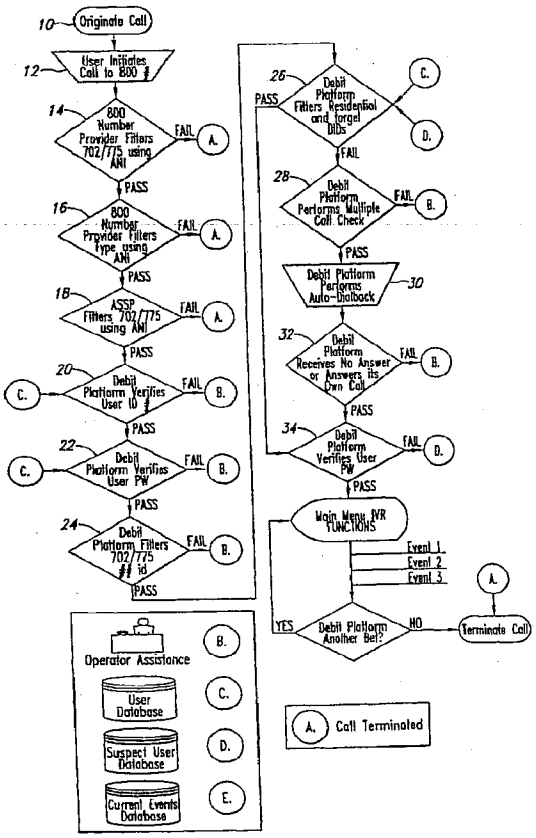
(74) Agent: BECKER, Todd, M.; Davis Wright Tremaine LLP, 2600 Century Square, 1501 Fourth Avenue, Seattle, WA 98101-1688 (US).

(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: PROCESS FOR SCREENING AND TRACKING USERS ON A TELEPHONIC NETWORK



(57) Abstract: A process for screening and monitoring users connecting or attempting to connect from a user platform to a target platform via a telephone network, the target platform being located within a specified jurisdiction. The process comprises filtering unauthorized calls from connecting to a target platform and writing call information for all calls connections made or attempted (step 12-18), verifying user identification (steps 20-34), and establishing a network connection between authorized callers and the target platform.

WO 00/54491 A1

Published:
with international search report

(48) Date of publication of this corrected version:
14 March 2002

(15) Information about Corrections:
see PCT Gazette No. 11/2002 of 14 March 2002, Section II

Previous Correction:
see PCT Gazette No. 14/2001 of 5 April 2001, Section II

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

PROCESS FOR SCREENING AND TRACKING USERS ON A TELEPHONIC NETWORK

FIELD OF THE INVENTION

The present invention relates to processes for screening and tracking user information on a telephone network, and more specifically to a process for screening and tracking users of a telephone wagering system.

BACKGROUND

Telephone networks pose a significant problem in the enforcement of federal and state gambling laws. Gambling is legal, although tightly regulated, in only two states (Nevada and New Jersey) and in limited areas within other states, such as Native American reservations. Electronic networks allow people residing in places where gambling is illegal to easily place bets with bookmakers in places where gambling is legal. This not only violates federal law against interstate gambling, but may violate laws of jurisdictions where gambling is otherwise legal.

Mechanisms for enforcing gambling laws for electronic networks have not kept pace with the technologies themselves: enforcement happens only after the fact in the rare cases when sufficient probable cause can be established to investigate and when the law-breaking gamblers can be tracked down or. No effective method has previously been devised of preventing the violation from occurring in the first place or, if a violation happens, no method of tracking the violation and whether it was intentional or accidental. Under the federal Racketeer Influenced Corrupt Organization (RICO), illegal gambling is established if the user is aware of the law, intentionally breaks the law (defined in RICO as doing the illegal act two or more times) and receives some form of consideration, for example a wager payout. No presently existing process tracks electronic wagering in the right ways and with sufficient detail such that RICO offenders can be prosecuted.

There is thus a need for a process that not only tracks illegal wagering for the purposes of prosecuting the offenders, but one that prevents persons from becoming offenders in the first place. The problem of preventing electronic gambling involves screening out those who, because their location, should not be gambling. It also involves tracking the users of the network

in such a way that, for example, people who unknowingly access the gambling part of the network will not be prosecuted for illegal gambling.

SUMMARY OF THE INVENTION

An inventive process is presented for screening and monitoring users connecting or attempting to connect from a user platform to a target platform via a telephone network, the target platform being located within a specified jurisdiction. The process comprises filtering unauthorized calls from connecting to the target platform, writing call information in a database for all connections made or attempted, and establishing a network connection between authorized callers and the target platform.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a flow chart which illustrates the overall process of screening users of a telephone wagering system.

Figure 2 shows a sample set of data saved by the process for each call. The data is used to track unauthorized use of the system.

Figure 3 shows the suspect user targeting matrix used to assign risk values to specific calls.

DETAILED DESCRIPTION OF THE INVENTION

An embodiment of the present invention is described below in the context of a wagering system accessible via a telephone network. The present invention, however, is capable of use with any type of platform connected to a telephone network to which access should be limited and tracked.

Figure 1 illustrates an embodiment of the screening process for screening users on a telephone network. The process is designed to ensure that a person authorized to access a regulated telephonic system is within a defined group, is within a geographically regulated region or is using an approved access medium. The process is also designed to collect data necessary to target, track and provide the means necessary to eliminate or investigate potential fraud or illegal attempts at accessing a regulated service. Multiple tiers or layers of security

provide redundancy, fault tolerance and adherence to the laws the system was designed to enforce like the Racketeer Influence Corrupt Organization (RICO) Act and the Kyle Act (also deemed the Communications Decency Act II).

In Figure 1, a user is attempting to establish a connection over the telephone network between their user platform and a target platform located in a jurisdiction, such as Nevada, where gambling is legal. In this embodiment the user platform is a telephone set, and the target platform is a regulated telephone wagering system. The process prevents calls originating from jurisdictions outside Nevada from accessing the wagering system, and also prevents calls from unauthorized locations within Nevada from accessing the wagering system. Additionally, the process can detect attempts to circumvent the law by using a callback feature. The process takes place at the carrier level, i.e., it takes place using the basic coding of the telephone network itself. It is not an application superimposed on top of the telephone network.

At steps 10 and 12, a user attempts to initiate a call to the telephone wagering system by dialing the telephone wagering system's assigned telephone number, which will usually be a toll-free "800" number supplied by the wagering system's telephone carrier. Whenever a user places a telephone call, the telephone switching equipment at the telephone company transmits a user identification code known as Automatic Number Identification (ANI) of origin taken from the user's Local Exchange Routing Guide. ANI is similar to caller ID, but ANI is carrier-based raw coded data contained in the Call Detail Report (CDR) transmitted with the telephone call. The ANI code is a string of digits comprising, among other things, the originating telephone set's area code, phone number, and information digits. The information digits consist of a two-digit code which identifies the origin of that call based on calling type, organization type or function type. Thus, the information digits indicate whether the telephone set is installed in a residence, a business, a government building, or is a mobile telephone such as a cellular or satellite phone. The detailed components of ANI and CDR are outlined in the publication *Local Exchange Routing Guide, General Information, Volume I* (Bell Communications Research, Dec. 1, 1998).

The first tier of security occurs at step 14, where calls originating outside the wagering system's jurisdiction are identified and terminated. This filtration is accomplished by parsing from the ANI of origin the area code where the user initiated the call. Once extracted, the area

code of the ANI of origin is checked against a stored list of approved area codes. Usually, these approved area codes will be all area codes within the jurisdiction where the wagering system is located. For example, in Nevada the 702 and 775 area codes (corresponding to Las Vegas and Reno, respectively) would be approved for access. If the area code of the user's ANI of origin is not on the approved list of area codes, the call is either terminated or forwarded to an operator. If the user telephone's area code is on the list of approved area codes, then the connection is allowed to proceed to the next security tier at step 16. Any calls that are terminated are logged in a call detail report in a suspect user database.

Step 16 is the next level of security, in which calls from unauthorized locations within the jurisdiction are identified and terminated. The law does not permit gambling from certain facilities, for example government buildings, so step 16 is designed to filter out calls originating from these locations. As discussed above, the user's ANI of origin contains a two-digit code (know as info digits) corresponding to the call type or organization type. At step 16, the process parses the info digits from the call's ANI of origin and compares them against a stored list of authorized info digits. If the call's info digits match those on the authorized list, the call originates from an authorized location and the connection is routed to step 18. If the call's info digits do not match those on the authorized list, the call does not originate from an authorized location and the connection is either terminated or forwarded to an operator, and the call information is recorded in a call detail report in a suspect user database.

Mobile user platforms, such as cellular or satellite telephones, require no additional steps beyond those outlined for step 14. Cellular telephone usually have an ANI code associated with the jurisdiction in which the phone was registered (i.e. the user's home area). But if a user makes a cellular telephone call while roaming, the ANI of origin is a temporary number issued by the telephonic switch servicing the call. This prevents a user from violating the gambling laws, as they must physically be present in the jurisdiction to gamble. For example, a user may have a cellular phone registered in Nevada, yet be located in California when attempting to place a call to the wagering system. As long as the user's call is serviced by a California telephone switch, the user will be unable to access the system.

At step 18 the call undergoes a redundant round of filtering identical to the filtering of steps 14 and 16. Step 18 checks whether the call originates inside the jurisdiction and whether the call originates from an authorized location within the jurisdiction. This redundancy is built into the system in case there is some sort or error or malfunction at steps 14 and 16.

The next security tier is step 20, where the user is asked to input their user identification number (user ID), which is a unique alphanumeric identifier assigned to a user when registering to use the wagering system. Under the law, only users previously registered with the wagering system can use the system. Once the user has input their user ID number, the process queries a user database to ensure that the input user ID is registered in the system. If the user ID is not in the database, the user's call is forwarded to an operator and logged in the call detail report database. If the user's identification is registered, the call proceeds to step 22.

Having entered their assigned user identification, the user next inputs a password at step 22. The user database is checked to ensure that the entered password corresponds to the user identification. If the password does not correspond to the user's ID, the call is forwarded to an operator. Otherwise, the call is forwarded to step 24.

At step 26, the process examines the info digits parsed from the ANI of the incoming call to assess whether the call is a high-risk call type that merits further anti-fraud verification. Calls originating from residential phones, for example, are suspect because it is difficult to trace the origin of a call forwarded through a residential phone number. Step 26 also checks the user's ANI information against ANI information of registered users and suspect users stored in databases C and D. If either the info digits or the user is identified as a high-risk type, the call is logged in the call detail report database and is either terminated or passed to the next level of security at step 28.

If a call fails the screening at step 26, then the next tier at step 28 checks for simultaneous connections to the system by the same ANI of origin, *i.e.* a forwarded phone call, or simultaneous connections under the same user identification. If a multiple connection is found, the call is terminated and the details of the call are stored in the call detail report on a suspect user database, with the user's risk code changed to identify the level of risk. The process of assigning risk codes is explained below.

At steps 30 and 32, the process performs an automatic dial-back to the user based on the info digit code (ANI) passed to it and the 800 number used to contact the platform. In the event of a forwarded call, for example, the call will be switched back to the wagering system; in essence it will be forwarded to itself. If found at step 32, these calls are logged in the Call Detail Report database with a risk rating indicating a "high suspect call" and the call is terminated. If the call passes the test at step 32, the call is passed to step 34, where the user's password is verified and the user is finally allowed access to the wagering system.

In addition to screening unauthorized calls as described above, the process also provides for tracking calls made to the wagering system to ensure compliance with the provisions of RICO and other laws. Figure 2 lists the 22 items of data kept in the suspect user database for each call made to the wagering system, whether successful or unsuccessful. Each item of data has a number corresponding to it.

The call information in the suspect user database is periodically processed and each unsuccessful call is assigned a risk rating according to the suspect user targeting matrix shown in Figure 3. In Figure 3, the numbers 13 through 22 in the top and left-hand columns correspond to data items 13 through 22 in the table of Figure 2. Risk ratings are assigned based on the frequency and characteristics of each unsuccessful call. The risk rating reflects the probability that a particular call was fraudulent.

If the process logs a single unsuccessful call from a particular ANI of origin, the process assumes that the call was simply a mistake on the part of the user and assigns the call a risk rating of zero. Once a second unsuccessful call is logged from a particular ANI of origin, the user is assigned a risk rating of 1, depending on how the call was terminated. For example, if the call was terminated because a callback found that calls were being forwarded (i.e. they are at the intersection of row 16 and column 16 because both connection attempts were from the same origin), then there are probably interstate calls going on and the call is assigned a risk rating of 2. Similarly, if the call was terminated because the info digits indicated that the call originated from a government building, then the call is probably intrastate and the call is assigned a risk rating of 1. Ratings of 4 and 5 are assigned to calls attempted three or more times based on statistical inference. The attempted calls are compared in both frequency and amount to 1.5 times the

standard deviation, and a risk rating of 4 or 5 is assigned depending on the confidence level resulting from comparing the calls to the statistical measures. A rating of 6 is assigned only when there are repeated calls at a confidence level of 97.5 % and there has been a wagering payout. At a risk factor of 6, fraud is almost certainly occurring.

At a user specified increment (minimum monthly), a "High Suspect Call" report is generated and individual reports on those calls can be generated. In the event of a caller appearing on the report, the individual chart generated by his multiple call attempts means that at least two attempts to penetrate the system have occurred and the probability of accident is greatly diminished. Using a statistical database engine, call comparisons are done against criteria specific to the type of target application the process is protecting. For example, in the telephone wagering system a suspect call must occur twice before becoming a suspect call and get a high risk rating. As origination, frequency of calls and dollar amount wagered vary from statistical means, confidence in the level of risk is raised as the deviation from the mean increases. The process becomes "smarter" as the sample size of the data set increases.

The screening and tracking process described is independent of the hardware used, and thus may be implemented using a variety of hardware. The first two steps (14 and 16) are carried out by the carrier's own telephone switching equipment. The remaining steps are preferably carried out by hardware comprising at least two T1 boards (one inbound, one outbound) programmed with basic telephonic functionality, including the ability to process ANI codes. It requires as a minimum one T1 line in and one T1 line out. At a minimum, these T1's are carrier coded with Automatic Number Identification (ANI), info digits, and destination number identification (DNIS). The telephone wagering system may be hosted by any compatible hardware.

The preferred method of setting up the hardware requires a P2 or above processor based server running any current network operating system, housing redundant processors, T1 boards, power supplies, disk drives in a level 5 raid array, tape backup unit (size determined by maximum user data expected over 18 month period), and a backup AC generator. The server is preferably connected to redundant T1's from 2 different local topologies of physical transport infrastructures. This configuration, along with client server access for database and statistical

engine administration with multi-tiered network security, should not suffer any downtime if any single hardware component fails. Server notification diagnostics should page a service technician prior to hardware failure, resulting in zero downtime.

CLAIMS

1. An automated process for screening and monitoring users connecting or attempting to connect from a user platform to a target platform via a telephone network, the target platform being located within a specified jurisdiction, comprising:

filtering unauthorized calls from connecting to the target platform;

writing call information in a database for all connections made or attempted;

establishing a network connection between authorized callers and the target platform.

2. The process of claim 1 wherein filtering unauthorized calls from connecting to the target platform comprises detecting attempted calls originating outside the jurisdiction and terminating the calls.

3. The process of claim 2 wherein filtering attempted connections originating outside the jurisdiction comprises:

extracting a user's automatic number identification (ANI) code transmitted by the user platform when the user attempts to call the target platform;

parsing an area code from the ANI, the area code identifying the jurisdiction in which the user platform is registered;

comparing the area code against a stored list of approved area codes; and

terminating the attempted connection if the user's area code is not on a list of approved area codes.

4. The process of claim 2 wherein filtering unauthorized calls from connecting to the target platform further comprises detecting attempted calls originating from unauthorized locations inside the jurisdiction and terminating the calls.

5. The process of claim 4 wherein filtering unauthorized calls from connecting to the target platform further comprises querying a database of authorized target platform users to assess whether the user is authorized to use the target platform.

6. The process of claim 4 wherein filtering attempted connections originating from unauthorized locations within the jurisdiction comprises:

extracting a user's automatic number identification (ANI) code transmitted when the user attempts to call the target platform;

parsing an originating facility code from the ANI, the originating facility code identifying the type of facility, the type of platform or the type of organization from which the attempted call originates;

comparing the originating facility code against a stored list of approved originating facility codes; and

terminating the attempted call if the originating facility code is not on the list of approved originating facility codes.

7. The process of claim 4 wherein the originating facility code indicates that the attempted connection originates from a mobile user platform, further comprising:

determining the physical location of the telephone switch servicing the mobile user platform based on an ANI assigned to the call; and

terminating the attempted connection if the mobile user platform is outside the jurisdiction.

8. The process of claim 4 wherein filtering unauthorized calls from connecting to the target platforms further comprises checking whether a user attempting to connect to the target platform has made multiple simultaneous attempts to connect to the target platform.

9. The process of claim 3 wherein filtering unauthorized calls from connecting to the target platform further comprises:

attempting to establish a confirming connection to the user platform; and

terminating the user's connection if a confirming connection to the user platform cannot be established.

10. The process of claim 9 wherein attempting to establish a confirming connection comprises:

attempting to establish a connection to the user platform using the user's UIC;

tracking the attempted connection to see whether the user's station is busy or whether the connection is routed back to the target platform.

terminating the call if the user station is busy or the connection is routed back to the target platform.

11. The process of claim 1 further comprising a process for tracking unsuccessful calls wherein tracking unsuccessful calls comprises:

assigning each unsuccessful call a risk code based on a set of rules and statistical inferences;

compiling statistics regarding the number of calls for each risk code, the statistics including the mean number of calls and the standard deviation.

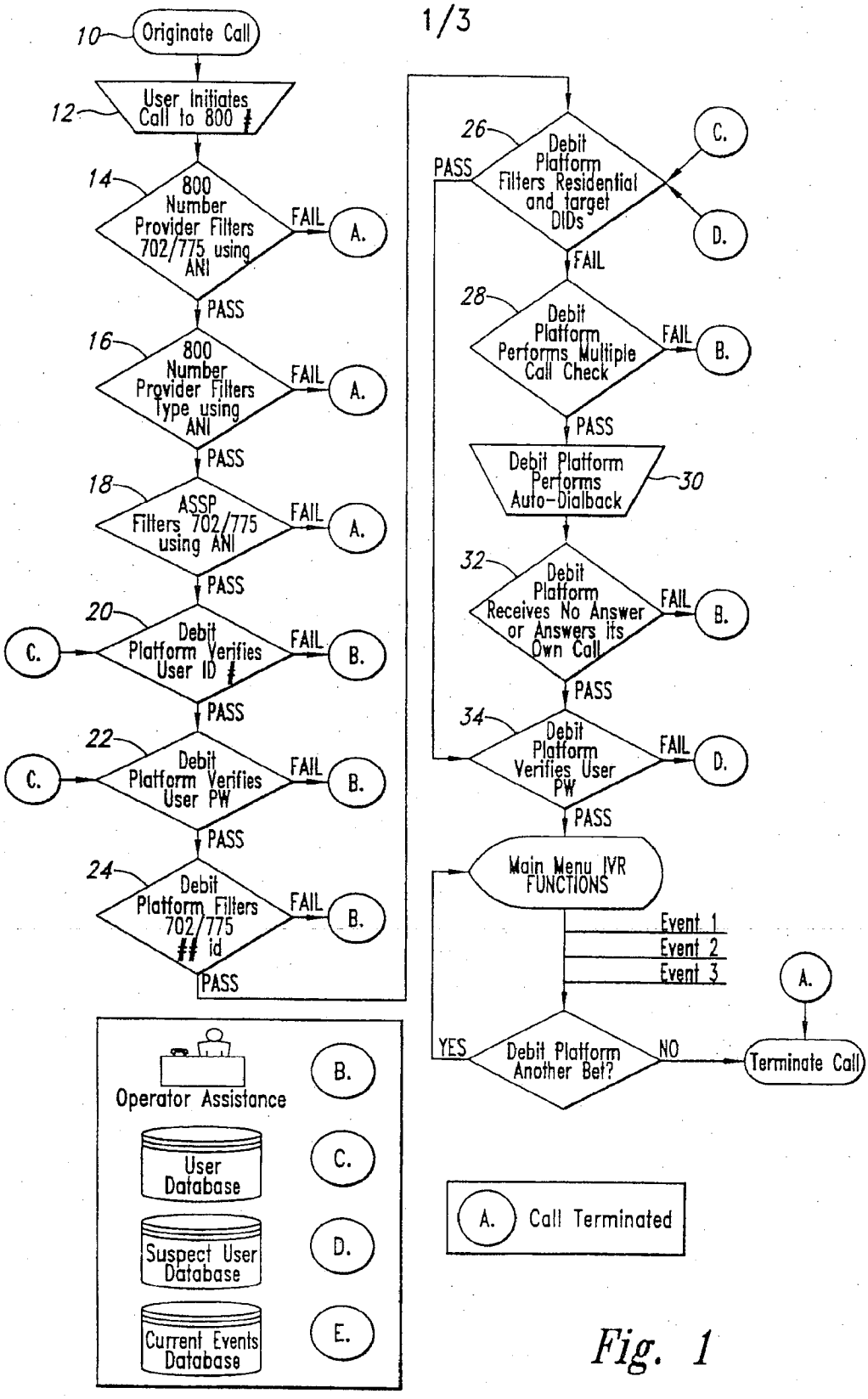


Fig. 1

1	User ID	Up to 20-Digit Numeric Field AZ
2	User Lname Fname MI	Up to 25-Digit Alphanumeric Field
3	User Street Address	Up to 25-Digit Alphanumeric Field
4	User City	Up to 25-Digit Alphanumeric Field
5	User Zip Code	Up to 6-Digits, no numbers
6	DNIS	10-Digit Numeric
7	User State	2-Digit Alphanumeric Field
8	User Registered Call Type (info)	2-Digit Number
9	Total Successful Connections	
10	Total Dollars Wagered *	
11	Total Dollars Paid *	
12	Average Call Length in Minutes	
13	Average Dollars Wagered Per Call *	
14	Total Concurrent Call Attempts	
15	Connection Attempts Different Origin	
16	Connections Attempts Same Origin	
17	Above Normal Successful Transactions	
18	Above Normal Average Call Length	
19	Above Normal Concurrent Call Attempts	
20	Above Normal Average Dollars Wagered *	
21	Above Normal Total Dollars Wagered *	
22	Total Winning Dollars Paid out on Wagers *	
	* Dependant on the IVR being up and fully operational	

Suspect User Targeting Matrix										
	13	14	15	16	17	18	19	20	21	22
14	0	1	3	4	4	5	6	6	6	
15	1	1	3	4	4	5	6	6	6	
16	3	3	2	4	4	5	6	6	6	
17	4	4	4	4	4	5	6	6	6	
18	4	4	4	4	4	5	6	6	6	
19	5	5	5	5	5	5	6	6	6	
20	6	6	6	6	6	6	6	6	6	
21	6	6	6	6	6	6	6	6	6	
22	6	6	6	6	6	6	6	6	6	

1	Possible Intra-State Cll Forwarding
2	Possible Inter-State Call Forwarding
3	Both 1 & 2
4	Increase in confidence to 75% probability
5	Increase in confidence to 92.5% probability
6	Possible Invalid Pay Out
X	Not Used

	High confidence of invalid betting occuring (greater than 75% chance of invalid betting)
X	Invalid betting is highly probable (92.5% chance invalid betting is occuring)
■	Money is being paid out on possible invalid betting

Fig. 2

Suspect User Targeting Matrix										
13	14	15	16	17	18	19	20	21	22	
14	0	1	3	4	4	5	6	6	6	
15	1	1	3	4	4	5	6	6	6	
16	3	3	2	4	4	5	6	6	6	
17	4	4	4	4	4	5	6	6	6	
18	4	4	4	4	4	5	6	6	6	
19	5	5	5	5	5	5	6	6	6	
20	6	6	6	6	6	6	6	6	6	
21	6	6	6	6	6	6	6	6	6	
22	6	6	6	6	6	6	6	6	6	

Fig. 3